UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/487,483	01/19/2000	Masue Shiba	04329.2217	3217

22852 7590 07/19/2006

FINNEGAN, HENDERSON, FARABOW, GARRETT & DUNNER
LLP
901 NEW YORK AVENUE, NW
WASHINGTON, DC 20001-4413

EXAMINER	
SIMITOSKI, MICHAEL J	

ART UNIT	PAPER NUMBER
2134	

DATE MAILED: 07/19/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	**Application No.** 09/487,483	**Applicant(s)** SHIBA ET AL.	
	Examiner Michael J. Simitoski	**Art Unit** 2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *04 May 2006*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *2-19* is/are pending in the application.

4a) Of the above claim(s) *11-19* is/are withdrawn from consideration.

5)☒ Claim(s) *2 and 5* is/are allowed.

6)☒ Claim(s) *3,4 and 6-10* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *30 March 2004* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date *4/11/06*.

4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) ☐ Notice of Informal Patent Application (PTO-152)

6) ☐ Other: _____.

DETAILED ACTION

1. The response of 5/4/06 was received and considered.

2. The IDS of 4/11/06 was received and considered.

3. Claims 2-19 are pending. As per the response of 5/4/06, claims 11-19 are withdrawn as being drawn to a non-elected invention.

Claim Rejections - 35 USC § 112

4. The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

5. Claims 3-4 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention.

Regarding claim 3, the specification does not describe two adder circuits as is claimed with one adder circuit in claim 2 and another in claim 3.

Regarding claim 7, the specification does not describe two full adders as recited with one adder in claim 6 and another in claim 7.

Regarding claim 8, the specification does not describe two full adders as recited with one adder in claim 6 and another in claim 8.

6. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

7. Claims 3-4 & 7-8 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Regarding claim 3, it is unclear if the adder circuit is the same as the adder circuit of claim 2 or a different adder circuit.

Regarding claim 3, "said integer unit arithmetic circuit" lacks proper antecedent basis.

Regarding claim 3, "said finite field GF(2^m) based unit arithmetic circuit" lacks proper antecedent basis.

Regarding claim 7, it is unclear if the full adder recited in the claim is an additional full adder or the same full adder as claim 6.

Regarding claim 7, it is unclear to which "full adder" the claim (line 4) is referring.

Regarding claim 8, it is unclear if the full adder recited in the claim is an additional full adder or the same full adder as claim 6.

Regarding claim 8, it is unclear as to which "full adder" the claim (line 4) is referring.

Regarding claim 8, it is unclear as to which result "the result" (line 5) is referring.

Claim Objections

8. Claim 8 is objected to because of the following informalities: "fuller adder" (line 2) should be replaced with "full adder". Appropriate correction is required.

9. Claim 9 is objected to under 37 CFR 1.75(c), as being of improper dependent form for failing to further limit the subject matter of a previous claim. Applicant is required to cancel the claim(s), or amend the claim(s) to place the claim(s) in proper dependent form, or rewrite the claim(s) in independent form. The limitations of claim 9 are presented in depending claim 6.

Claim Rejections - 35 USC § 102

10. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

11. Claims 6-10 are rejected under 35 U.S.C. 102(e) as being anticipated by U.S. Patent 6,230,179 to Dworkin et al. (**Dworkin**).

Regarding claim 6, Dworkin discloses an arithmetic unit/arithmetic processor (col. 3, lines 24-32) including an integer unit arithmetic circuit (col. 7, lines 12-18 & 36-46), wherein the arithmetic circuit comprises a full adder (Fig. 8, #170), the full adder including a carry propagation section configured to propagate a carry of an operation result (Fig. 8, #182) of the full adder upon reception of a selection signal (Z/F_2^M) corresponding to an integer-based unit arithmetic operation (col. 7, lines 42-43 & lines 60-62) and to not propagate the carry of the full adder upon reception of a selection signal (Z/F_2^M) (col. 7, lines 42-43 & lines 60-62) corresponding to a finite field GF(2^m)-based unit arithmetic operation and a controller configured to output, to said integer unit arithmetic circuit, a selection signal (Fig. 8, Z/F_2^M) for selecting one of an integer unit arithmetic operation and finite field GF(2^m)-based unit arithmetic operation wherein an integer-based multiply operation (col. 7, lines 13-22) or a finite field GF(2^m)-based multiply operation (col. 4, lines 58-67) is selected by controlling the carry propagation (col. 7, lines 42-43 & lines 60-62).

Regarding claim 7, Dworkin discloses wherein said integer unit arithmetic circuit comprises a full adder (Fig. 8, #170), and said carry propagation controller comprises a switch (Fig. 8, #160) to which the selection signal (Fig. 8, Z/F_2^M) and a carry out signal/m_j are input, and performs carry propagation control of said full adder in units of bits (col. 4, lines 29-34).

Regarding claim 8, Dworkin discloses wherein said integer unit arithmetic circuit comprises a full adder (Fig. 8, #170), and said carry propagation controller comprises a selection section (Fig. 8, Z/F_2^M) configured to switch between outputting a 2-input EX-OR result (Fig. 8, #160) obtained by said full adder in units of bits and outputting an EX-OR result based on the result and an input carry as an addition result (Fig. 8, #160).

Regarding claim 9, Dworkin discloses wherein said integer based unit arithmetic circuit adds by propagating a carry when executing the integer based multiply operation (col. 7, lines 42-46) and adds without propagating any carry when executing the finite field GF(2^m) based multiply operation (col. 7, lines 42-46 & lines 60-62).

Regarding claim 10, Dworkin discloses a crypto processing apparatus for selectively encrypting or decrypting based on an integer based operation said arithmetic apparatus defined in claim 6, and encrypting or decrypting based on a finite field GF(2^m) based arithmetic operation by said arithmetic apparatus (col. 1, lines 26-39).

Allowable Subject Matter

12. Claims 2 & 5 are allowed.

Regarding claim 2, U.S. Patent 6,230,179 to **Dworkin** discloses an arithmetic unit/arithmetic processor (col. 3, lines 24-32) comprising an integer based multiplier circuit (col. 7, lines 12-18 & 36-46), a finite field GF(2^m)-based multiplier circuit (col. 5, lines 11-12 & 33-34) and an adder circuit (Fig. 5, #54) shared by the separated integer based multiplier circuit and the finite field GF(2^m)-based circuit (col. 5, lines 32-41) and configured to operate on data from either the integer based multiplier or the finite field GF(2^m)-based multiplier circuit (col. 3, lines 28-32) and a controller for controlling said selector to make said selection (col. 3, lines 28-32). U.S. Patent 6,3.97,241 to **Glaser** teaches logically adjacent but separate integer and finite field circuits (Fig. 1), but not sharing an adder. Japanese Unexamined Patent (publication 5/28/1999) 11-143688 to **Okada** was cited by Applicant in a paper dated 4/11/06 and discloses performing RSA and elliptic curve cryptography (¶27 & Fig. 1). However, the prior art relied upon fails to teach or suggest an integer based multiplier circuit and a finite field GF(2^m)-based multiplier circuit logically adjacent but separated from said integer based multiplier circuit and an adder circuit shared by the separated integer based multiplier circuit and the finite field GF(2^m)-based multiplier circuit.

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. The Dupaquis reference is cited for teaching performing two separate operations (integer and finite field) and extracting the products from one and the Elbe reference is cited for teaching a carry-disabling signal (abstracts).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Michael J. Simitoski whose telephone number is (571) 272-3841. The examiner can normally be reached on Monday - Thursday, 6:45 a.m. - 4:15 p.m..

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Jacques Louis-Jacques can be reached on (571) 272-6962. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

MJS

June 20, 2006

JACQUES LOUIS-JACQUES
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100